



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/222,846	12/30/1998	KAZUOMI OISHI	35.G2331	2585

5514 7590 01/25/2005

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER

CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application N .

09/222,846

Applicant(s)

OISHI

Examiner

Paul Callahan

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,6,7,10-14,18-20 and 22-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,6,7,10-14,18-20 and 22-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10-19-2004 has been entered.

2. Claims 1-3, 6, 7, 10-14, 18-20, and 22 were pending at the time of the previous Office Action in the case. New claims 23-28 have been added via the latest amendment. Therefore claims 1-3, 6, 7, 10-14, 18-20, and 22-28 are now pending and have been examined.

Response to Arguments

3. Applicant's arguments filed 10-19-2004 have been fully considered but they are not persuasive.

The Applicant argues in traverse of the rejections of claims 1, 10, 14, 18, 20, and 22 that the combination of Hickman and Ryan fails to teach an image processing apparatus. However a careful reading of the references reveals that both do indeed teach an image processing apparatus. Ryan teaches such an image processor by virtue of the system being one that undertakes communications authentication processing between elements of a postal evidencing

Art Unit: 2137

and distribution system. Such systems typically involve optical scanning and processing of postal indicia.

The applicant attempts to distinguish the instant invention from the Ryan '473 reference by noting that in Ryan, only the unencrypted form of the key is erased and the encrypted form of the key is maintained in the database. However, the form of the key that is used in the image processing is indeed erased in Ryan, and is not stored. Therefore Ryan does teach this feature of the applicant's claimed invention.

The applicant states that: "Moreover, Ryan is not seen to disclose anything with regard to the apparatus inputting digital information encrypted with the encryption key stored in the external source, obtaining, from the external source, a decryption key corresponding to the encryption key, and decrypting the input encrypted digital information by using the obtained decryption key. However a careful reading of Ryan reveals that such is indeed taught at col. 4 lines 52-55.

The Applicant argues in traverse of the taking of Official Notice that the step of using a high-efficiency coding algorithm prior to encryption of image data is old and well known in the art. The Applicant asks for a showing of art demonstrating that such is indeed an obvious step. The Applicant's attention is now drawn to Enari, US 5,933,499, fig. 5 items 24, and 26 where a high-efficiency coding algorithm is applied to such data prior to encryption.

The remainder of the applicant's arguments are moot in light of the revisions made to the language of the claims by the latest amendment and the consequent revisions to the formulation of the rejections of the claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3, 6, 7, 10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman et al. US 5619015, in view of Ryan Jr. et al., US 6192473.

As for claims 1, 10, and 14, Hickman teaches an image input apparatus comprising (abstract): reading means for reading an encryption key stored in an external source (col. 5 lines 5-10: Image data used as an encryption Key); storage means for storing said read encryption key to execute an encryption process (col. 5 lines 5-10, fig. 6: "Microprocessor"); encryption means for encrypting digital information with said encryption key stored in the storage means (col. 5 lines 5-10); output means for outputting the encrypted digital information (col. 5 line 11); erasing means for erasing said encryption key stored in said storage means after encrypting the digital information by said encryption means (col. 5 lines 11-12). Ryan teaches the features of claim 1 not taught by Hickman, namely an input means for inputting digital information encrypted with said encryption key stored in said external source (col. 4 lines 52-55); obtaining means for obtaining, from said external source a decryption key corresponding to said encryption key (col. 4 lines 52-55); and decryption means for decrypting the input encrypted digital information by using said decryption key obtained by said obtaining means (col. 4 lines 52-55). Therefore it

Art Unit: 2137

would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Ryan into the system of Hickman. Motive to make this combination may be found for example in col. 4 lines 29-35 of Ryan where the advantage of erasing private or secret keys used in such a communications system is discussed.

As for claims 3 and 12, Hickman teaches An image input apparatus according to claim 1, further comprising image pick-up means for optically picking up an image of a subject and for generating an image signal from the image (fig. 6 item 34).

As for claim 6, Hickman does not teach the use of a key wherein said encryption key comprises an encryption key based on a common key cryptosystem. However Ryan does teach this step (col. 4 line 63 where a symmetric session key is used to encrypt the data). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Ryan into the system of Hickman. It would have been desirable to do so as this would allow for rapid decryption of the received encrypted data. Motive to make this combination may be found for example in col. 3 lines 59-67 of Ryan where the utility of such a symmetric key communication system is discussed.

As for claims 7 and 13, Hickman does not teach an image input apparatus according to claim 1, wherein said encryption key comprises an encryption key based on a public key cryptosystem. However Ryan does teach the use of a public key system in col. 4 lines 48-58. Therefore it would have been obvious to one of ordinary skill in the art at the time of the

Art Unit: 2137

invention to incorporate this feature of Ryan into the system of Hickman. Motive to make this combination may be found for example in col. 3 lines 59-67 of Ryan where the utility of such a public key communication system is discussed.

6. Claims 2 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman and Ryan as applied to claim 1 above, and Official Notice. The combination of Hickman and Ryan fails to teach an image input apparatus according to claim 1, wherein said encryption means encrypts the digital information that has undergone a high-efficiency coding operation. However Official Notice may be taken that the use of such high-efficiency coding operations in the transmission of encrypted image data is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system. It would have been desirable to do so as this would decrease the bandwidth required for transmission of the encoded, encrypted data.

7. Claims 18-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ryan in view of Schneier, "Applied Cryptography 2nd Edition," Oct. 1995.

As for claims 18, 20, and 22, Ryan teaches an image input apparatus (col. 3 line 25: "Postage Evidencing System") comprising: generating means for generating an internal key (col. 3 lines 36-39, col. 4 lines 17-19), information encryption means for encrypting digital information with said internal key (col. 4 lines 15-20); reading means for reading an external encryption key stored in an external source (col. 4 lines 10-13: public key certificate obtained from certificate authority); storage means for storing said external encryption key to execute a

Art Unit: 2137

key encryption process (col. 4 lines 24-26); output means for outputting the encrypted digital information and the encrypted internal encryption key (col. 4 lines 24-26); and erasing means for erasing said external encryption key and said internal encryption key after executing said encryption process by said information encryption means and said key encryption means (col. 4 lines 26-35); input means for inputting encrypted digital information and an encrypted internal key (col. 5 lines 12-25); obtaining means for obtaining an external decryption key corresponding to said external encryption key stored in said external source (col. 5 lines 12-25); key decryption means for decrypting said input encrypted internal key with said obtained external decryption key (col. 5 lines 12-25), and decryption means for decrypting said input encrypted digital information with said internal key decrypted by said key decryption means (col. 5 lines 12-25). Schneier teaches the features of claim 18 that Ryan fails to teach, namely a key encryption means for encrypting said internal encryption key with by using said external encryption key stored in said storage means (page 51: Public Key Cryptosystem). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Schneier into the system of Ryan et al. Motive to make this combination is found in page 51 of Schneier where the utility of delivery of a session key via a public-key protocol in performing functions such as digital signature verification is discussed. Ryan discusses digital signature verification as a function of the Key Management System in col. 5 lines 12-25).

As for claim 19, Ryan teaches an image input apparatus according to claim 18, wherein said internal encryption key comprises an encryption key based on a common key cryptosystem (col. 4 lines 17-19). Ryan does not teach an external encryption key that comprises an encryption

key based on a public key cryptosystem. However Schneier teaches this feature (page 51: Public Key Cryptosystem). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have incorporated this feature of Schneier into the system of Ryan et al. Motive to make this combination is found in page 51 of Schneier where the utility of delivery of a session key via a public-key protocol in performing functions such as digital signature verification is discussed. Ryan discusses digital signature verification as a function of the Key Management System in col. 5 lines 12-25).

8. Claims 23-25, 27 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman and Ryan as applied to claims 1, 10, and 14 above, and further in view of Laing et al. US 5,534,857. The combination of Hickman and Ryan does not teach an image input apparatus according to Claim 1, wherein the external source comprises an integrated circuit card irremovably connectable to the image input apparatus and the encryption and decryption keys are stored in the integrated circuit card. However Laing does teach this feature (fig. 3 item C1). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hickman and Ryan. It would have been desirable to do so as this would allow for portable storage and more secure refreshing of the keys needed by the KMS and SOHO servers of Ryan.

9. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ryan and Schneier as applied to claims 18, above, and further in view of Laing et al. US 5,534,857. Laing teaches the features of claim 26 that the combination of Ryan and Schneier fails to teach, namely

Art Unit: 2137

an image input apparatus according to Claim 18, wherein the external source comprises an integrated circuit card irremovably connectable to the image input apparatus and the encryption and decryption keys are stored in the integrated circuit card (fig. 3 item C1). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Hickman and Ryan. It would have been desirable to do so as this would allow for portable storage and more secure refreshing of the keys needed by the KMS and SOHO servers of Ryan.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

1/18/05

*Paul Callahan**Andrew Caldwell*

**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**